



IT Security Handbook

Access Control -

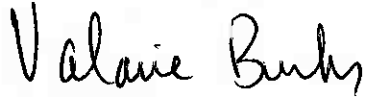
ITS-HBK-2810.15-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.15-01)
Access Control

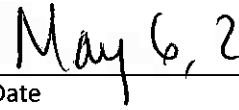
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History	3 -
1 Introduction and Background	5 -
2 Account Management (AC-2)	5 -
3 Access Enforcement (AC-3)	6 -
4 Information Flow Enforcement (AC-4)	6 -
5 Separation of Duties (AC-5)	6 -
6 Least Privilege (AC-6)	6 -
7 Unsuccessful Login Attempts (AC-7)	7 -
8 System Use Notification (AC-8)	7 -
9 Concurrent Session Control (AC-10)	7 -
10 Session Lock (AC-11)	7 -
11 Permitted Actions without Identification or Authentication (AC-14)	7 -
12 Remote Access (AC-17)	8 -
13 Wireless Access (AC-18)	8 -
14 Access Control for Mobile Devices (AC-19)	8 -
15 Publicly Accessible Content (AC-22)	9 -
16 Elevated Privileges	9 -
17 Organizationally Defined Values	11 -

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.1 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Access Control (AC) information security controls.
- 1.2 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.3 - The Access Control security control family relates to the ability of NASA to permit or deny access to computer systems, system locations and system information based on a user's need to know. The control family encompasses the management of unique account identifiers (IDs), passwords, physical access, badges and tokens, and user permissions to ensure the proper level of system access.
- 1.4 - **Applicable Documents**
- *NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology*
 - *NPD 2810.1, NASA Information Security Policy*
 - *NPR 2810.1, Security of Information Technology*
 - *NPR 2841.1, Identity, Credential, and Access Management*
 - *NASA EA-STD-0001. Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorizations Infrastructure*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-0035, Digital Media Sanitization*
 - *ITS-HBK-2810.15-02, Managed Elevated Privileges (EP)*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-46, Guide to Enterprise Telework and Remote Access Security*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
 - *NIST SP 800-121, Guide to Bluetooth Security*
 - *HSPD-12, Policies for a Common Identification Standard of Federal Employees and Contractors*

2 Account Management (AC-2)

- 2.1 - **Roles and Responsibilities**

- 2.1.1 *The Center Chief Information Officer (CIO) shall:* -
 - 2.1.1.1 - Review and approve waivers for granting elevated privileges to users without the requisite training in accordance with *ITS-HBK-2810.15-02*. -
 - 2.1.1.1.1 - The Center CIO may delegate the responsibility for the review and approval of waivers to the Center Information Security Official (CISO) or other NASA staff, but not to the account issuer. -
 - 2.1.1.1.2 - Waivers shall not exceed 90 days, and should include justification for its provisions. -
- 2.1.2 *The Information System Owner (ISO) shall:* -
 - 2.1.2.1 - Identify account types (e.g., security roles, user privilege groups) for NASA users of their information systems in the NASA Access Management System (NAMS). -
 - 2.1.2.2 - Identify conditions necessary to be granted identified account types, in NAMS. -
 - 2.1.2.3 - Require appropriate approvals for requests to establish accounts (including any training requirements) in NAMS. -
 - 2.1.2.4 - Authorize and monitor the use of guest/anonymous/temporary accounts. -
 - 2.1.2.4.1 - Guest and anonymous accounts should only be used when the content and services being accessed are public in nature. -
 - 2.1.2.4.2 - Temporary accounts should be provisioned through NAMS. -
 - 2.1.2.5 - Ensure the timely deactivation of accounts which are no longer needed, and accounts of terminated or transferred users. -
 - 2.1.2.5.1 - Integration with the NASA Consolidated Active Directory (NCAD) provides automation of this function. -
- 2.1.3 *The NAMS Project Manager shall:* -
 - 2.1.3.1 - Establish procedures for the authorization, establishment, activation, modification, disabling, and removal of accounts in NAMS. -
 - 2.1.3.2 - Ensure the capability to automatically disable temporary, emergency, and inactive accounts. -
 - 2.1.3.3 - Notify the Security Operations Center (SOC) or appropriate organization (e.g., Center-specific IT Security office, incident response team, or help desk) of any NAMS workflows used to manage the authorization of accounts with elevated privileges. -
 - 2.1.3.3.1 - All NAMS workflows used to manage elevated privileges should require: -
 - a. - Business Justification: This should explain a user's need for elevated privileges, and list the specific activities for which the privileges will be used.
 - b. - Periodic review in a manner consistent with organizationally defined values for account review frequencies.

3 Access Enforcement (AC-3)

- 3.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

4 Information Flow Enforcement (AC-4)

- 4.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

5 Separation of Duties (AC-5)

- 5.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

6 Least Privilege (AC-6)

6.1 - Roles and Responsibilities

- 6.1.1 *The ISO shall:* -

- 6.1.1.1 - Ensure users of information systems are assigned access authorizations only to the degree necessary to carry out - their responsibilities. -
- 6.1.1.2 - Approve the provision of administrator access, and elevate privileges for their information systems in accordance - with *ITS-HBK-2810.15-02*. -

7 Unsuccessful Login Attempts (AC-7)

7.1 - Roles and Responsibilities

7.1.1 *The ISO shall:* -

- 7.1.1.1 - Ensure the capability to enforce appropriate system access limitations as a result of unsuccessful login attempts in - a manner consistent with organizationally defined values. -

8 System Use Notification (AC-8)

8.1 - Roles and Responsibilities

8.1.1 *The ISO shall:* -

- 8.1.1.1 - Ensure the display of the System Use Notification, as defined by *NPR 2810.1*, on any information system which - includes an interactive login interface. -
 - 8.1.1.1.1 - An information system shall maintain display of system use notifications and prevents further access, until explicit - action is taken by the user to accept all terms and conditions. -
 - 8.1.1.1.2 - This applies to all computers and applications that are owned or operated on behalf of NASA and require user - authentication for access. -
- 8.1.1.2 - Ensure that the appropriate warning banner, as defined by *NPR 2810.1*, is displayed on NASA resources or - information systems utilizing NASA networks until explicit action is taken by a user to accept all terms and - conditions. This includes any information system components: -
 - 8.1.1.2.1 - On a network whose addresses are assigned to NASA; -
 - 8.1.1.2.2 - That processes NASA data (public or non-public); -
 - 8.1.1.2.3 - That is actively or potentially managed by or on behalf of NASA; or -
 - 8.1.1.2.4 - That is actively or potentially monitored by or on behalf of NASA. -

8.1.2 *The NASA User shall:* -

- 8.1.2.1 - Agree to the an appropriate use policy statement based on *NPD 2540.1* and approved by the NASA General - Counsel, prior to being granted access to any NASA information system. -

9 Concurrent Session Control (AC-10)

9.1 - Roles and Responsibilities

9.1.1 *The ISO shall:* -

- 9.1.1.1 - Ensure the capability to limit the number of concurrent sessions on an information system in a manner consistent - with organizationally defined values. -

10 Session Lock (AC-11)

10.1 - Roles and Responsibilities

10.1.1 *The ISO shall:* -

- 10.1.1.1 - Ensure the capability to lock a user session following a determined length of inactivity in a manner consistent with - organizationally defined values. -

11 Permitted Actions without Identification or Authentication (AC-14)

- 11.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

12 Remote Access (AC-17)

12.1 Roles and Responsibilities

12.1.1 *The ISO shall:*

12.1.1.1 Ensure only devices that are authorized and approved for remote access to the information system to which they are connecting are granted remote access in a manner consistent with organizationally defined values.

12.1.1.1.1 National Security or classified information shall not be processed, stored, or transmitted on personally-owned or third-party devices at any time.

12.1.1.2 When employing multifactor authentication for remote access to information systems, ensure that it is *NIST SP 800-63* Level 4 compliant using the PIV card, or RSA SecurID.

12.1.1.2.1 2-factor identification using the PIV card or RSA SecurID shall be required for remote access to non-privileged accounts.

12.1.1.3 Ensure that remote access is routed through NASA network access control points.

12.1.2 *The NASA User shall:*

12.1.2.1 Use only NASA authorized and approved devices for remote access to NASA non-public information systems.

12.1.2.2 If teleworking, have a telework agreement in place.

12.1.2.3 Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely (e.g., not leaving laptops and other devices unattended or in public plain view).

12.1.2.4 Understand their responsibilities for protecting Personally Identifiable Information (PII) data, and the consequences for mishandling PII.

13 Wireless Access (AC-18)

13.1 Roles and Responsibilities

13.1.1 *The Center CISO shall:*

13.1.1.1 Provide the capability to scan for unauthorized wireless systems.

13.1.1.2 Ensure unauthorized wireless systems are disabled and reported immediately to the SOC or appropriate organization (e.g., Center-specific IT Security office, incident response team, or help desk).

13.1.1.3 Ensure the scanning of information systems for unauthorized wireless access points or otherwise posing risk to NASA information systems, in a manner consistent with organizationally defined values.

13.1.2 *The ISO shall:*

13.1.2.1 Ensure that only wireless systems that meet approved authentication protocols are used for Local Area Networks (LAN) or as access points to NASA information systems.

13.1.2.2 Ensure a risk analysis with consideration to the guidelines of *NIST SP 800-121* is conducted prior to the use of Bluetooth technologies for NASA devices.

14 Access Control for Mobile Devices (AC-19)

14.1 Roles and Responsibilities

14.1.1 *The ISO shall:*

14.1.1.1 Ensure that only NASA approved and authorized mobile devices are used to access non-public NASA information systems.

14.1.1.1.1 Approved and authorized mobile devices are those devices that are purchased and owned or contracted for use by NASA government or contract employees (e.g., Outsourcing Desktop Initiative for NASA (ODIN) devices, NASA IT Infrastructure Improvement Program (I3P) devices).

14.1.1.2 Ensure that mobile devices carried on travel to locations where there is concern for the loss or compromise of NASA sensitive information are examined upon return for physical tampering.

- 14.1.1.3 Ensure that all disk media for mobile devices carried on travel to locations deemed to be of significant risk are sanitized in accordance with *ITS-HBK-0035* and re-imaged, if required, upon return.

15 Publicly Accessible Content (AC-22)

15.1 Roles and Responsibilities

15.1.1 *The ISO shall:*

- 15.1.1.1 Review new content on publicly accessible information systems, and monitor for any information which may not be approved for public release in a manner consistent with organizationally defined values.
- 15.1.1.2 Remove immediately any information deemed to be not approved for public release from any publicly accessible information system.

16 Elevated Privileges

- 16.1 More detailed information on the requirements for requesting, implementing, and managing elevated privileges may be found in *ITS-HBK-2810.15-02*, Managed Elevated Privileges (EP) Implementation Handbook.

16.2 Roles and Responsibilities

16.2.1 *The Center CISO shall:*

- 16.2.1.1 Review and approve/deny all requests for elevated user privileges.
- 16.2.1.2 Maintain authority to approve requests for elevated privileges on all NASA information systems which reside at their Center, or whose system security plans are managed at their Center.
- 16.2.1.3 Verify that qualification requirements have been met before approving a request for elevated user privileges.
- 16.2.1.4 Maintain the ability to revoke elevated privileges.

16.2.2 *The ISO shall:*

- 16.2.2.1 Ensure that all information system users with elevated privileges have been authorized to hold those privileges.
- 16.2.2.2 Ensure that elevated privileges are granted only to those users who are qualified to access the information system.
- 16.2.2.3 Ensure that elevated privileges are used only for the purposes for which they were granted.
- 16.2.2.4 Maintain the ability to revoke elevate privileges.

16.2.3 *The Information System Security Officer (ISSO) shall:*

- 16.2.3.1 Periodically review and validate that only authorized accounts have elevated privileges.
- 16.2.3.2 Ensure that elevated privileges are used only in a form consistent with the usage justification.
- 16.2.3.3 Maintain the ability to revoke elevated privileges.

16.2.4 *The NASA User shall:*

- 16.2.4.1 Meet the following requirements In order to qualify for elevated privileges:
 - 16.2.4.1.1 Renew all applicable SATERN training and/or maintain all relevant industry certifications.
 - 16.2.4.1.2 Demonstrate knowledge of the following topics: (Note: The following may be demonstrated through the completion of SATERN certification for elevated privileges)
 - a. The risks of accessing a computer with elevated privileges, to the information stored on the computer, to the computer itself, and to other NASA devices in the same environment.
 - b. Best practices and precautions to be used when accessing an information system with elevated privileges.
 - c. User responsibilities associated with accessing a NASA information system with elevated privileges.
 - d. Ramifications of user actions when accessing a NASA information system with elevated privileges.
- 16.2.4.2 If granted elevated privileges for a period exceeding 30 days, demonstrate knowledge of the following topics: (Note: The following may be demonstrated through the completion of SATERN "IT Security for Systems Administrators, Beginner Level" certification)

ITS Handbook (ITS-HBK-2810.15-01) -
Access Control -

- 16.2.4.2.1 - Incident Response (including identifying potential incidents; knowing how, when, and to whom to report potential or actual incidents; knowing how to recover from an incident).
 - 16.2.4.2.2 - Security Program Management Compliance (including understanding the purpose of and elements of the - Information Security Program; applying Information Security Program elements to the information system; - identifying areas of weakness in the Information Security Program). -
 - 16.2.4.2.3 - Security components of each phase in the System Development Life Cycle (SDLC) (including knowing which security controls to implement and how; recognizing weakness in a security control; recognizing if the security controls are not implemented according to the implementation plan; understanding security ramifications of changes to a system; knowing how to modify security controls to accommodate changes in operations; understanding that each system impacts the security of other systems that it is being connected to; knowing the information security responsibilities of users of the information system; monitoring information systems to identify potential information security incidents; understanding and meeting all data retention and disposal requirements; etc.).
 - 16.2.4.3 - Use elevated privileges only for the purposes for which they were granted.
- 16.2.5 *The System Administrator shall:*
- 16.2.5.1 - Meet all requirements of a NASA User in seeking elevated privileges.
 - 16.2.5.2 - Demonstrate knowledge of the following: (Note: The following may be demonstrated through the completion of SATERN "IT Security for Systems Administrators, Intermediate Level")
 - 16.2.5.2.1 - Incident Response (including making decisions on whether policy has been breached and if further action is - needed). -
 - 16.2.5.2.2 - Security Program Management Compliance (including interpreting compliance with NASA's IT Security Program and analyzing patterns of non-compliance).
 - 16.2.5.2.3 - Security components of each phase in the SDLC (including analyzing system performance and approving system configuration and functionality; assessing, understanding, and interpreting performance of security controls and their effect on changes on security vulnerabilities; identifying new vulnerabilities; assessing security controls' ability to correct new vulnerabilities, and applying new or modified controls; knowing how to accommodate operational changes and maintain an acceptable level of risk; understanding procedures to follow for actual security incidents; knowing how to apply NASA security policy to the disposal of information and systems and how to decide on the best way to dispose of assets no longer in use; knowing how to conduct proper archiving, sanitizing, or disposition of all hardware, software, data, and facility resources; etc.).

17 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
AC	01	Access Control Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
AC	02	Account Management	Main	[1]	Frequency	Account reviews.	2/Year	2/Year	2/Year
AC	02	Account Management	E 2	[1]	Reference	Emergency/temporary account termination.		30 Days	30 Days
AC	02	Account Management	E 3	[1]	Time Period	Automatic inactive account disabling.		60 Days	60 Days
AC	06	Least Privilege	E 1	[1]	Reference	List of security functions and information for which there is explicit authorization for access.		a. System administration. b. Establishing system accounts. c. Configuring Access authorizations (i.e. permissions; privileges). d. Setting events to be audited. e. Setting intrusion detection parameters.	a. System administration. b. Establishing system accounts. c. Configuring Access authorizations (i.e. permissions; privileges). d. Setting events to be audited. e. Setting intrusion detection parameters.

ITS Handbook (ITS-HBK-2810.15-01) -
Access Control -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
AC	06	Least Privilege	E 2	[1]	Reference	List of security functions and information for which a user with access would need another non-privileged account or role to perform other system functions.		a. System administration. b. Establishing system accounts. c. Configuring Access authorizations (i.e. permissions; privileges). d. Setting events to be audited. e. Setting intrusion detection parameters.	a. System administration. b. Establishing system accounts. c. Configuring Access authorizations (i.e. permissions; privileges). d. Setting events to be audited. e. Setting intrusion detection parameters.
AC	07	Unsuccessful Login Attempts	Main	[1]	Number	Consecutive, invalid login attempts before automated account locking.	5 Attempts	5 Attempts	5 Attempts
AC	07	Unsuccessful Login Attempts	Main	[2]	Time Period	Time box on consecutive, invalid login attempts before automated account locking.	15 Minutes	15 Minutes	15 Minutes
AC	07	Unsuccessful Login Attempts	Main	[3]	Selection	Automatic action.	Lock account/node for a defined time period.	Lock account/node for a defined time period.	Lock account/node for a defined time period.
AC	07	Unsuccessful Login Attempts	Main	[3] [1]	Time Period	Automatic account/node locking.	15 Minutes	15 Minutes	15 Minutes
AC	07	Unsuccessful Login Attempts	Main	[3] [2]	Reference	Next login delay algorithm.	No Delay (Per FDCC)	No Delay (Per FDCC)	No Delay (Per FDCC)
AC	10	Concurrent Session Control	Main	[1]	Number	Concurrent same-user session limits.			1 Session/User
AC	11	Session Lock	Main	[1]	Time Period	Inactive session locks (for VPN/SNA connections using FIPS 140-2 validated encryption).	15 Minutes	15 Minutes	15 Minutes
AC	17	Remote Access	E 5	[1]	Frequency	Monitoring of unauthorized connections.		1/Week	Continuous

ITS Handbook (ITS-HBK-2810.15-01) -
Access Control -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
AC	17	Remote Access	E 7	[1]	Reference	List of security functions and information for which additional security measures are needed.		a. Establishing system accounts. b. Configuring access authorizations. c. Performing system administration functions. d. Auditing system events or accessing event logs.	a. Establishing system accounts. b. Configuring access authorizations. c. Performing system administration functions. d. Auditing system events or accessing event logs.
AC	17	Remote Access	E 7	[2]	Reference	Additional security measures.		FIPS 140-2 validated encryption of all transmitted data.	FIPS 140-2 validated encryption of all transmitted data.
AC	17	Remote Access	E 8	[1]	Reference	Disabled, unsecure network protocols.		Peer-to-Peer (P2P)	Peer-to-Peer (P2P)
AC	18	Wireless Access	E 2	[1]	Frequency	Unauthorized wireless connection scans.			4/Year
AC	19	Access Control for Mobile Devices	Main	[1]	Reference	Mobile device dispositioning following travel to locations of significant risk. (Note: All foreign travel is considered a "significant risk").	Hard drive purge and re-image.	Hard drive purge and re-image.	Hard drive purge and re-image.
AC	22	Publically Accessible Content	Main	[1]	Frequency	Review of content for non-public information.	1/Week	1/Week	1/Week